# BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

## IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.**

(12) UK Patent Application (19) GB (11) 2 229 020 (13) A

(43) Date of A publication 12.09.1990

(21) Application No 8907987.5

(22) Date of filing 10.04.1989

(30) Priority data
(31) 8905044 (32) 06.03.1989 (33) GB

(51) INT CL[5]
G06F 12/14

(52) UK CL (Edition K)
G4A AAP

(56) Documents cited
GB 2168831 A EP 0242808 A1 EP 0165789 A2
EP 0067611 A1 WO 83/02343 A1

(58) Field of search
UK CL (Edition J) G4A AAP
INT CL[4] G06F

(71) Applicant
Chris Kelron Ellis
Clive Vale, Old Perry Street, Northfleet, Kent,
DA11 8BT, United Kingdom

(72) Inventor
Chris Kelron Ellis

(74) Agent and/or Address for Service
Chris Kelron Ellis
Clive Vale, Old Perry Street, Northfleet, Kent,
DA11 8BT, United Kingdom

# (54) Security device to limit remote access to computers over a telecommunication network

(57) The device is an independent unit with a timer, memory and random password generator, able to store, generate, recognise and transmit passwords; store and transmit telephone numbers and recognise and retransmit permitted signals. Telephone numbers, passwords and signals may only be programmed into the device when a key is inserted into the unit and a suitable input device used. As the unit is able to effect call back procedures and recognise certain signals and retransmit them independently of the computer it protects the potential hacker is never able to gain access to the protected computer. The call back and signal screening (indirect access) function may be used jointly or independently.

GB 2 229 02

# SECURITY DEVICE TO LIMIT REMOTE ACCESS TO COMPUTERS OVER A TELECOMMUNICATION NETWORK

This invention relates to the control of remote access to computers over a telecommunication network.

The practice of 'computer-hacking', the gaining of unauthorised access to a computer by persons typically using their own computer linked through a modem to a telephone network, has been of growing concern to businesses and governments over recent years. The conventional way of protecting computer systems from such access is by the use of one or more passwords. Hackers, however, have shown themselves expert in guessing, discovering or using computer programs to find the correct password. Once a hacker has gained access to a computer system the intruder is often able to view, alter or erase private data, disrupt the normal functioning of that system and put in place a 'back-door'. A 'back-door' is a set of instructions which tell the computer to admit the hacker when he or she uses a particular code, regardless of any changes to the normal passwords.

This invention seeks to exclude hackers from any access to the computer system, so that they are unable to attempt the computers password sequence or gain any other access, regardless of whether or not a 'back-door' has been installed into the system.

According to the present invention there is provided a unit with an independent memory and capable of receiving and recognising certain identification and communication signals over the telecommunication network used. The unit is capable of generating its own identification signal and random password; able to generate dialling sequences or initiating dialling sequences directly or indirectly to effect contact with other users of the telecommunications network. The unit which may or may not be free standing, will only allow access to or by the computer system it protects over the telecommunications network after it has effected certain security procedures such as or similar to those described under the specific embodiment of the invention below. The call back procedures are designed only to allow access to the computer by authorised users whose details have been pre-programed into the unit. The indirect access procedure is designed to limit the instructions that may be

communicated to the computer once contact has been established. Although described together below, it is envisaged that for certain security applications either the call back procedures or the indirect access procedure would alone be appropriate. In these cases, to reduce costs, units may be supplied which are only able to perform the appropriate tasks.

A specific embodiment of the invention will now be described as if the telecommunications network is to be the British Telecom telephone system. The unit has a memory containing a library of identification signals it recognises, together with the telephone numbers of the authorised users of those signals and the units own identification signal. When the indirect access procedure is to be used, the memory also contains a list of those commands the computer may accept from each user or group of users. Alterations to this library may only be made when the correct key is inserted into a lock in the unit, turned and remains within the unit. Such alterations may be made by an input device, such as a keyboard, which may be integral or external to the unit. The unit also has a random password generator, a timing unit and memory to store certain details of calls made to or from

other network users, such as the identification signal of the unit or other system contacted or contact received from and any random password transmitted or received which will be recorded for a limited time. In addition, the unit has a longer term memory to record details of calls made and received, their time, duration and the identification of those contacted or contact received from. When the unit's key is in place, this information may be output via an integral or external output device, such as a printer, and that part of the memory may be erased. This memory may also be used to report the current operational state of the unit.

The call back security procedure the unit is designed to effect is as follows:

Case One — When the unit receives a call from a user of the telecommunications network who is not using a similar unit it will receive and record the identification signal transmitted by the calling network user, then it will cut or otherwise cause to be cut the communication line. Once the caller has disconnected, or has been disconnected, the unit will call the

number in its library corresponding to the identification signal received. When the connection is made the unit will then allow the computer it protects direct or indirect access to the communication line. If, however, the identification received is not recognised the unit will not attempt to make any call and will not allow connection to the computer it protects. If the unit calls the number in the library and it contacts a system giving an identification other than that of the original caller no connection will be made.

Case Two

When the unit receives a call from a user of the telecommunications network who is using a similar unit it will record both the identification signal and the random password transmitted. The calling unit will then cut the telephone line. The unit having received the call will then call the telephone number in its library corresponding to the identification signal received. It will transmit its own identification signal and the random password it recorded, which it will

then erase from its memory. Assuming the unit so contacted had placed the original call within its pre-programed time limit, both units will connect their computers directly or indirectly over the telephone line. If, however, the identification received is not recognised the unit will not attempt to make any call and will not allow connection to the computer it protects. If the unit calls the number in the library and it contacts a system giving an identification other than that of the original caller no connection will be made.

If the unit whose identification was given did not place the call or did place the call but the call back was not achieved within a pre-set time limit, no connection of either computer to the telephone lines will be made.

Case Three — The unit is instructed to call an authorised user who does not have a similar unit. The unit telephones the number in its library corresponding to the user it has been asked to contact. When it has exchanged identification signals with the computer it has contacted, having confirmed it is the correct machine, it will connect its computer directly or indirectly to the telephone line.

Case Four — The unit is instructed to call an authorised user who does have a similar unit. The unit telephones the number in its library corresponding to the user it has been asked to contact. When it has exchanged identification signals with the unit it has contacted, having confirmed it is the correct machine, it will generate and transmit a random password. It will then cut the telephone line. For a limited time the unit will remember both the identification signal of the machine it called and the random password. If the machine called then calls

back and gives its identification signal and the random password within a pre-set time limit the unit will allow access, either directly or indirectly to its computer. If the return call does not come within the time allowed the unit will erase its memory of the password. If the return call then comes the unit will treat it as if it were an instruction to call an authorised user who has a similar unit and repeat the steps of 'Case Four' from the beginning.

When the access the unit is programmed to allow to the computer is indirect the unit will only recognise and pass on those incoming instructions or pattern or sequence of instructions which it has been pre-programed to accept from that particular authorised user. The unit would not interfere with the transmissions made by the computer it protects.

The indirect access feature would be especially useful when the computer protected contains, for example, a large data-base. Different users could be allowed to access varying amounts or sections of information. Instructions which might, for instance, alter the computers programming or access restricted data would not be recognised by the unit and therefore not be passed onto the computer where they could be processed.

When the unit is used to enforce the indirect access procedure without the call back procedure in operation, the unit would be unable to differentiate between users. In this case it would apply a single library of acceptable pre-programed instructions or pattern or sequence of instructions to all telecommunication network users.

CLAIMS

1. A computer security device with its own memory independant of the computer it protects, connected between the computer and the telecommunications network.

2. A computer security device as claimed in Claim 1, able to store generate, recognise and transmit passwords, store and transmit telephone numbers (or other telecommunication identification signal) to effect a pre-set identification and call back procedure.

3. A computer security device as calimed in Claim 1 or Claim 2, able to store, receive and recognise certain signals signals, retransmitting only those which it is programed to permit.

4. A computer security device as claimed in any preceding claim, with an internal modem or similar device.

5. A computer security device as claimed in any preceding claim, mounted internally to the computer casing.

6. A computer security device as claimed in any preceding claim, sharing a power source with the computer or other hardware.

7. A computer security device as claimed in any preceding claim, with an input device secured by a mechanical or electronic locking device.

NB The word 'signals' in claim 3 was typed twice in error.